AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* TARGET ACCOUNTS, more fully described in Attachment A	)	Case No. MJ20-023

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

TARGET ACCOUNTS, more fully described in Attachment A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 U.S.C. §§ 2261A; 876(c); 371	Stalking; Mailing Threatening Communications; Conspiracy

The application is based on these facts:

✓ See Affidavit of Special Agent Michael Stults continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Michael Stults, FBI Special Agent

Printed name and title

◉ The foregoing affidavit was sworn to before me and signed in my presence, or
○ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: January 17, 2020

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

USAO# 2018R00225

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Michael Stults, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the FBI, currently assigned to investigate domestic terrorism in the Seattle Field Office and have been so employed for 2 years. My experience as an FBI Agent includes the investigation of cases where individuals frequently utilize computers and the Internet to coordinate and facilitate various crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training on network and information security, and on the methods and tactics of open source intelligence gathering.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (the "**TARGET ACCOUNTS**") that are stored at premises controlled by an electronic communications service and remote computer service provider. The information to be searched is described in the following paragraphs and in Attachments A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC, located at 1600 Amphitheater Parkway, Mountain View, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B, pertaining to the following accounts, identified in Attachment A:

cmrnShea18[@]gmail.com ("TARGET ACCOUNT #1")

Any account linked to MEID 256691624201282613 / IMSI 310120254586077 ("TARGET ACCOUNT #2")

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

In this affidavit, I have bracketed portions of email addresses discussed in this affidavit to ensure that they are not inadvertently hyperlinked and activated by anyone reading an electronic copy of this document. Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B.

3. As described below, CAMERON BRANDON Shea, aka "KROKODIL," is the user of **cmrnShea18[@]gmail.com (TARGET ACCOUNT #1)** and any account linked to **MEID 256691624201282613 / IMSI 310120254586077 (TARGET ACCOUNT #2)**. Based on the review of evidence obtained through this investigation, this application seeks a search warrant for both of the **TARGET ACCOUNTS** for certain records and information, including content, from **July 1, 2019, to the present**.

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2261A (Stalking); 876(c) (Mailing Threatening Communications); and 371 (Conspiracy) have been committed by known and unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes, as described in Attachment B.

APPLICABLE LAW

6. Title 18, United States Code, Section 2261A provides for criminal penalties for whoever:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

> with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that--
>
> (A) places that person in reasonable fear of the death of or serious bodily injury to a person, . . . described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A).

7. The persons described "in clause (i), (ii), (iii), or (iv) of paragraph (1)(A)" are:

> (i) that person;
>
> (ii) an immediate family member (as defined in section 115) of that person;
>
> (iii) a spouse or intimate partner of that person; or
>
> (iv) the pet, service animal, emotional support animal, or horse of that person.

8. Title 18, United States Code, Section 876(c), provides for criminal penalties for:

> Whoever knowingly so deposits or causes to be delivered as aforesaid, any communication with or without a name or designating mark subscribed thereto, addressed to any other person and containing any threat to kidnap any person or any threat to injure the person of the addressee or of another

9. Title 18, United States Code, Section 371 prohibits conspiring to commit a federal offense, and taking an overt act in furtherance of the conspiracy.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF PROBABLE CAUSE

A. Overview

10. The FBI is conducting an investigation into Cameron Brandon Shea, an individual living in Woodinville, Washington. Shea is a high-level member and primary recruiter for the Atomwaffen Division (AWD). AWD came to the attention of law enforcement on or about May 12, 2017 when Devon Arthurs was arrested for murdering two of his roommates near Tampa, Florida. Arthurs had been a member of AWD, as were his roommates. After his arrest, Arthurs admitted to the murders of his two roommates and told investigators he had committed the murders after he had converted to Islam and that the murders were his attempt at keeping the members of AWD from committing planned acts of terror related to the group's ideology. Arthurs claimed AWD had plans to use explosives to damage infrastructure and to use firearms to commit acts of violence.

11. After Arthurs' arrest, another roommate, Brandon Russel, who was the leader of AWD, was encountered by law enforcement at the residence unharmed. In the residence, law enforcement found bomb-making precursor chemicals and hexamethylene triperoxide diamine, a high explosive chemical. Russell admitted the chemicals were his and, on or about May 20, 2017, Russell was charged in a federal criminal complaint in Florida with a violation of Title 26, United States Code, Section 5861(d) (possession of an unregistered destructive device) and Title 18, United States Code, Section 842(j)(unlawful storage of explosive material). In addition to the explosive material inside the residence, law enforcement discovered Nazi paraphernalia and a framed image on the wall in honor of Oklahoma City bomber, Timothy Mcveigh.

12. Following the arrest of Russell, AWD selected John Denton, a resident of Houston, Texas, and Kaleb J. Cole, aka Khimaere or Khim, a resident of Arlington, Washington, to co-lead AWD in Russell's absence. Members of AWD also formed a relationship with Denver, Colorado resident, James Mason, who is the writer of the book, "Siege," which serves as the basis for AWD ideology. The book, which is a collection of neo-Nazi newsletters authored by Mason, advocates the leaderless resistance and lone offender

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

strategies as a viable means to accelerate the collapse of the system which members of AWD believe to be controlled by Jews.

13. On January 25, 2018, AWD hosted a "Death Valley Hate Camp" in Las Vegas, Nevada, where members trained in hand-to-hand combat, firearms, and created neo-Nazi propaganda videos and pictures of themselves posing with weapons. Cole coordinated the camp, beginning planning in early October 2017. Cole traveled from Washington State to Las Vegas for the hate camp with another Washington State AWD member, Aidan Bruce-Umbaugh. The two possessed concealed pistol licenses and transported numerous firearms and cases of ammunition to the event. California AWD member Samuel Woodward was expected to be at this hate camp, but could not attend due to being arrested for the murder of Blaze Bernstein who was an openly gay Jewish college student.

14. Prior to YouTube removing their pages, AWD posted propaganda videos on two channels called "AWDTV" and "Atomwaffen Division." One of those videos titled "Zealous Operation," depicts a hate camp at Devil's Tower, an abandoned cement factory in Concrete, Washington. Approximately half a dozen AWD members can be seen wearing military style clothing, face masks, and carrying an assortment of long guns, while conducting paramilitary style training and shooting at a gravel pit attached to Devil's Tower. At the beginning of the video participants state, "*GAS THE KIKES! RACE WAR NOW*!" while the statement is spelled out at the bottom of the screen.

15. On February 23, 2018, *The Seattle Times* published an article discussing AWD, and identifying several of its members nationwide, to include some in Washington State. Photographs, along with personally identifiable information, including home and work addresses, were included in the article. The article also discussed the application Discord that members used to facilitate communication. According to the article, several thousand pages of Discord chat logs between members were hacked and leaked to the public. After having been identified, several of the AWD members, to include those in leadership positions, deleted their online profiles, quit their jobs, changed residences, and moved to the Swiss-based, encrypted electronic communication service Wire, in an attempt to go dark and avoid detection by law

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

enforcement. Cole was one of the AWD members identified in this article, but Shea's involvement in the group was not reported.

16. Based on confidential human source (CHS) reporting, on or about September 16, 2018, Cole posted a recorded leadership message to AWD members via Wire. In the recording, Cole said, "*The matter of these nosy reporters coming into our daily lives, where we work, where we live, where we go in our spare time. We must simply approach them with nothing but pure aggression. We cannot let them think that they can just… that that it's safe for them to just come up to us, and fuck with us. We cannot let them think they are safe in our very presence alone….*"[1] The statement was in response to an incident where journalist AC Thompson confronted Denton at a music festival in Texas for the "*Documenting Hate"* news series.

17. Investigation into the group had identified Krokodil as a Washington based member who was the primary recruiter for AWD. Krokodil was also active in other online forums such as Gab and FascistForge.com, where he espoused racial violence, and stated how he and other members could "*go full McVeigh and start dispatching political and economic targets today, helping build the social tension that will accelerate the collapse of the system.*" Krokodil had also been planning to attend a November 2018 AWD Hate Camp being held in western Washington state, but was ultimately unable to attend due to medical reasons. Investigation later positively identified the user of the Krokodil moniker was Shea based on physical surveillance, consensual video recordings, and records demonstrating ownership of his phone number.

18. On July 9, 2019, Cole was interviewed by the FBI when he was deported from Canada to the United States. During the interview, Cole blamed the media for sensationalizing information about AWD and expressed dismay as to why he was targeted by the media in their stories, and how he was never approached in an attempt to collect accurate information. Cole felt the media's reporting of AWD being a threat to the public was "*internet nonsense*."

[1] The quotations from the members of the conspiracy in this Affidavit were captured by CHS reporting.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. In August of 2019, leadership members of AWD attended a "Nuclear Congress" in Las Vegas, Nevada, where members gave presentations, discussed recent events, challenges, plans going forward, and operational security. Shea discussed the importance of keeping identity protected, and how the media continues to be a challenge to AWD.

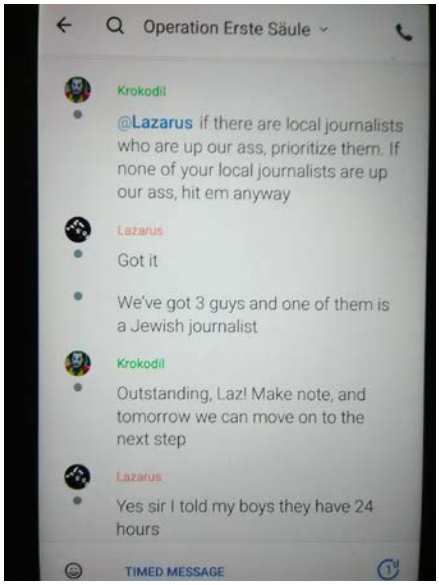
20. On September 26, 2019, Cole was served with an Extreme Risk Protection Order (ERPO) by the Seattle Police Department (SPD). SPD and Arlington Police Department officers seized 9 firearms in Cole's possession, as well as a number of unfinished lower rifle receivers, capable of being milled into functional rifle components with the equipment Cole owned. In the wake of the ERPO service, several news outlets nationwide covered the event. Source reporting covered Shea, Cole, and other AWD members discussing and disparaging the media coverage of the event, with one member suggesting to "*hit back… embarrass the enemy on their own front*."

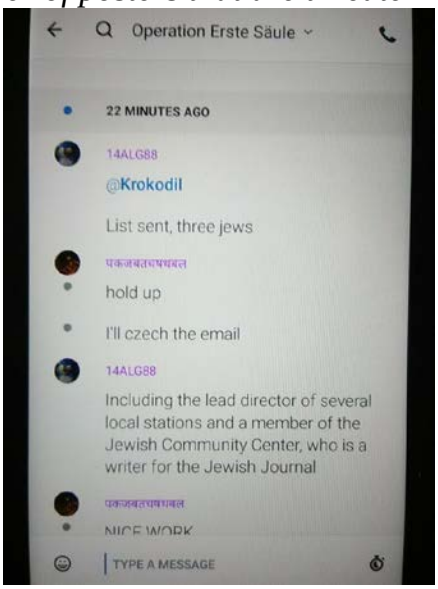
21. On November 4, 2019, Cole and Bruce-Umbaugh were stopped by law enforcement for speeding in Post, Texas while on their way to meet with Denton, near Houston, Texas. Bruce-Umbaugh was subsequently arrested for 18 USC 922 (g)(3) (Possession of a Firearm by an Unlawful User of a Controlled Substance). Law enforcement seized four firearms and approximately 2000 rounds of ammunition. Cole continued to the Houston area to meet with Denton.

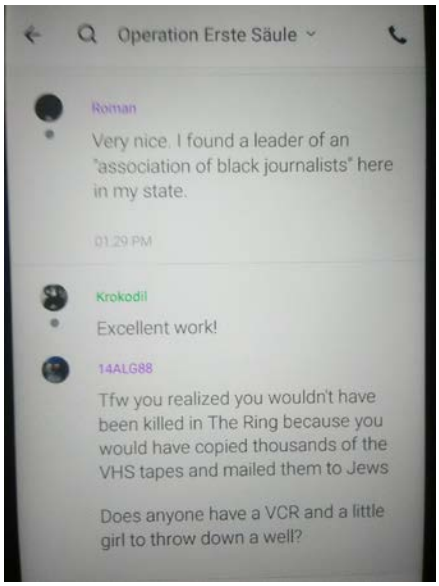
22. Per CHS reporting, in or about November 2019, Shea, using the moniker Krokodil, established a private Wire chat group titled, Operation Erste Saul. Shea invited co-conspirators to this chat group to collaborate on an effort to target journalists' homes and media buildings. According to Shea, the purpose of the operation was to "*send a clear message that we [AWD] to have leverage over them… The goal of course, is to erode the media/states air of legitimacy by showing people they have names and addresses and hopefully embolden others to act as well*." Other Participants in the chat group included Cole, Alexander Gosch, using the handle 14ALG88, an unknown person using Lazarus, an unknown person using Roman, and others. Shea directed each participant to identify, research, and locate journalists in their area. Lazarus reported that his cell had three targets, and one was

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Jewish. Gosch advised his cell was targeting three Jews. Roman said he found a leader of an association of black journalists in his state. Shea stated that the identification of these targets was "*Excellent work!*" and "*Outstanding.*" Shea wrote that the AWD cells in Florida, California, and Oregon had already acquired approximately 12 targets including home addresses, and that one of the targets was a "*cultural center.*" Shea went on to state that Khim [Cole] was, "*developing a number of posters that are threatening but not explicitly.*"



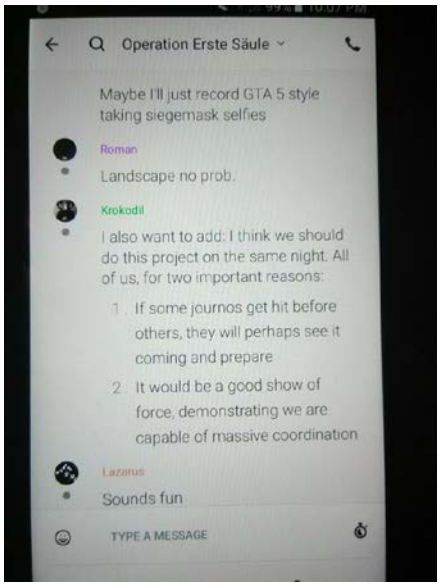


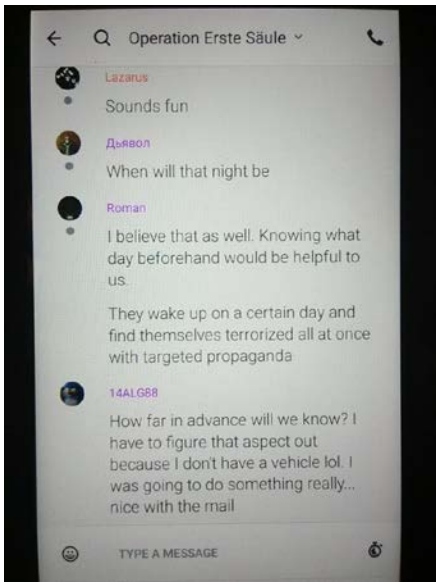


23. During this same discussion, Shea requested that co-conspirators email information about the targets to him within 24 hours at the email address atomtvjhfie8hjh4s[@]secmail.pro. Secmail.pro is a Finnish based company known for its privacy and security centric email service. Shea further explained that the information would be placed into custom posters for the targets. Cole stated that newer AWD initiates whose identity was not known to the public would carry out Operation Erste Saule. Shea indicated the he too would participate in carrying out the operation because his identity was not known to the public.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

24. On or about December 11, 2019, during a continued discussion to coordinate Operation Erste Saule, Shea explained that he wanted to coordinate the operation on the same night so journalists would be caught off guard, and to accomplish an effective "*show of force, demonstrating we are capable of massive coordination*." Roman discussed the intended impact of the coordinated plan was to "*have them all wake up one morning and find themselves terrorized by targeted propaganda.*" Cole also suggested buying rag dolls and knives, so one could leave a doll knifed through the head, at their target location.

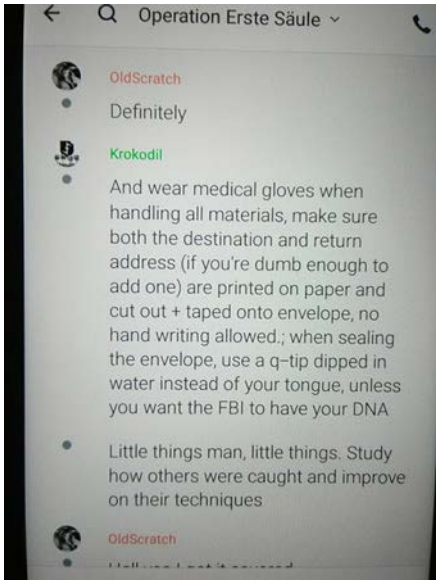


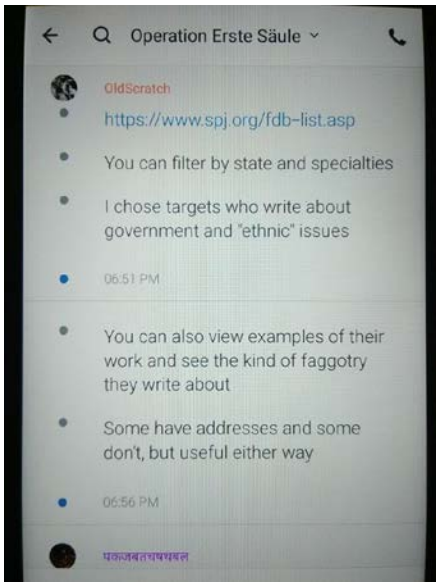


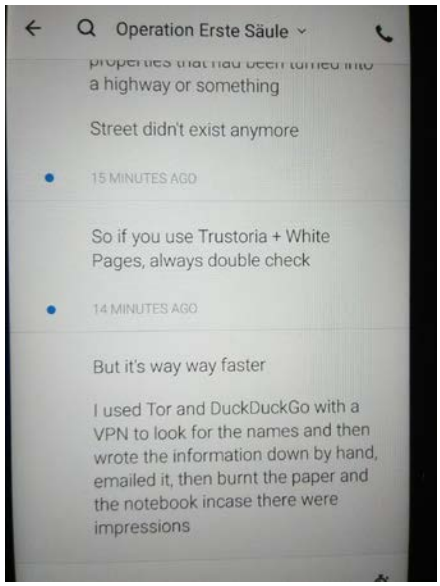
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

25. On or about December 11, 2019, during a Wire discussion to coordinate Operation Erste Saule, Cole told his co-conspirators that the group was working on getting more addresses, and the posters. Cole suggested that his co-conspirators conduct reconnaissance of their victims' addresses and suggested searching their addresses in Google maps. Cole told his co-conspirators to use, "*proper electronic opsec measures*," which I believe describes an intent to anonymize or privatize their actions to avoid law enforcement and obfuscate any activity.

26. On or about December 18, 2019, during a Wire discussion to coordinate Operation Erste Saule, Cole explained that he had addresses from Washington, Oregon, California, Ohio, and Florida. Shea wanted everyone to respond within 48 hours before moving on to the next stage. Co-conspirators discussed how to print propaganda posters. Shea discussed operational security in terms of buying stamps in another town with cash while wearing a disguise. Shea also recommended using a mailbox with no cameras and to wear medical gloves to avoid prints or DNA. Another AWD member, Roger Rowe, aka Oldscratch, recommended using the website [https://www.spj.org/fdb-list.asp], to acquire victim addresses. This URL contains a list of journalists and their contact information for the SOCIETY OF PROFESSIONAL JOURNALISTS.







UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. On or about December 25, 2019, during a Wire discussion to coordinate Operation Erste Saule, Cole explained that he was going to distribute the posters via "Guerrila Mail" with the subject line, "*prop-run*." Guerrila Mail is an electronic communication service that offers temporary, disposable email accounts. On or about December 26, 2019, during a Wire discussion to coordinate Operation Erste Saule, Cole confirmed that everyone in the group had received their propaganda poster. An unknown person using the moniker Azazel provided his email address as xogofi1993[@]mailart.top, and confirmed he was in the same cell as an unknown person using the moniker Lazarus. Azazel and Lazarus are believed to be members of a Florida chapter of AWD. An unknown person using the moniker Roman asked when they were going to execute the operation. Shea, Cole, and Azazel continued discussion to coordinate a date to execute Operation Erste Saule.

28. On or about December 27, 2019, during a Wire discussion to coordinate Operation Erste Saule, Shea decided to execute the operation on January 25, 2020. Cole wanted AWD members to take video of their activities. An unknown person using the moniker Roman said was, "*scoping my places on maps right now*." Oldscratch indicated one of his targets was in a gated community. Roman discussed using a disguise such as wearing construction gear to blend in, or to execute the operation at night. Shea discussed using his bicycle to avert being detected by license plate readers. Roman stated how the operation was going to deliver a "*nationwide scare*."

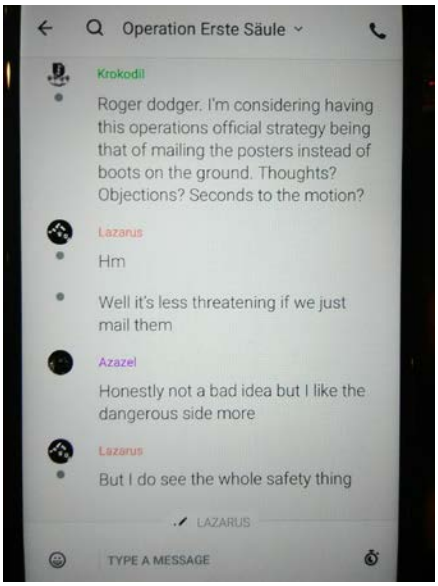
//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

29. On or about January 6, 2020, during a Wire discussion to coordinate Operation Erste Saule, Shea stated his cell was, "*air tight… ready to go…*" Members again discussed the coordination of the operation and opinions on conducting the operation entirely via the mail. Lazarus stated "*it is less threatening if we just mail them*." Shea and others ultimately decided to stay with "*boots on the ground*" at some locations and mailing them to the riskier target locations. Shea emphasized operational security, stressing the importance of not getting caught and remaining invisible to law enforcement.



30. Cole referenced multiple times in the chat group that he was the individual designing and creating the posters. On or about December 26, 2019, Cole stated he "*sent the posters out*" and that he had been "*having issues with my linux machine.*" Based on my training and experience, I understand a "linux machine" to be a personal computer utilizing the linux operating system. The posters sent to the group were directed to be mailed or posted to the home addresses of targeted journalists. All three of the posters contain threatening statements and insinuations, indicating the targets are under surveillance and at risk from AWD and contain a blank area at the bottom designated for placement of the specific target address.

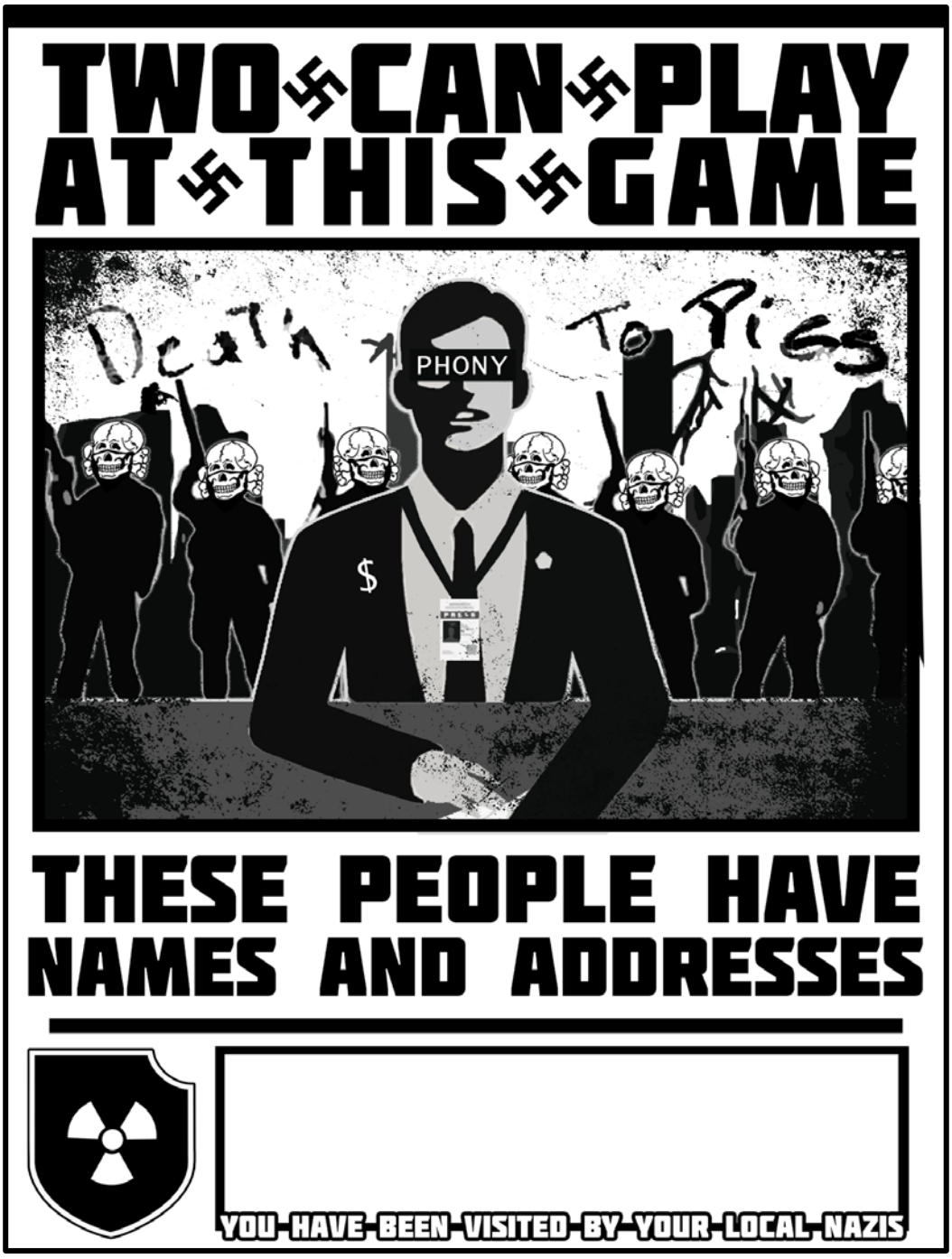
31. Based upon the group's own statements, Cole's prior statements about media intimidation, and the nature of the Operation Erste Saule as explained by Shea, I believe Shea,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Cole, and co-conspirators intend for the following posters, produced by Cole, to intimidate their respective targets, and given the nature of the prospective targets and the circumstances of Operation Erste Saule as outlined by Shea, these posters would cause fear, intimidation, and substantial emotional stress of their respective targets. The posters are attached hereto and made a part hereof by this reference.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



32. On or about January 7, 2020, Shea stated to his co-conspirators: *"If we are arrested later in connection to the operation, but they can't prove we specifically did it, fedwaffen's open sourcing of the AW brand name gives us plausible deniability…And since we*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

have JM's [Mason] disavowal of fedwaffen on the website, saying we disavow illegal action, that further helps our point that fedwaffen was behind this." It is known to investigators that "fedwaffen" is a reference to a faction of unknown individuals who have in recent months, posted AWD videos and propaganda online, claiming to be AWD. However, this new unsanctioned faction and all its communications were disavowed by Mason and members of the real AWD.

B. Shea's Involvement and Use of The TARGET ACCOUNTS

33. As discussed herein, the FBI, through its investigation, has identified numerous members of Atomwaffen Division, including Shea, who have planned and conspired to implement a targeted campaigned with the goal of terrorizing journalists with threatening propaganda.

34. Through the investigation, Shea was identified as the leader of the operation, who was actively aware of, and participating in all communication and planning leading to the execution of their plan. Shea's involvement includes:

a. On or about December 4, 2019, Shea, using his online moniker "Krokodil," created the "Operation Erste Saule" private chat group in the WIRE application. Shea then invited several other AWD affiliates into the private group. The chat group was established and utilized for the planning and coordination of executing the targeted propaganda campaign.

b. A main element of the operation was the identification of and research into the personal identifiable information of journalists in a member's respective area. Based on my training and experience, someone conducting internet research on an individual would begin with querying names and other known information about a target within an Internet search service, such as Google, the largest and most popular Internet search engine available. Shea detailed to the group the concern over being captured or identified on any sort of surveillance equipment a target's home might have. Shea stated he would "*google security camera systems*" in order to familiarize themselves with the types of home surveillance available, what they look like, and any possible weaknesses they may have. Based on my

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

training and experience, it is likely that if Shea is suggesting group members utilize the Google search engine to conduct research, he himself utilized Google to plan or research facets of this operation. It is known to the investigators that the **TARGET ACCOUNTS** are Google accounts actively used by Shea, and capable of capturing the search query and browser histories of utilized Google services.

c. An additional method of research discussed was public information database services, such as Whitepages.com. Based on financial records and subpoena returns, Shea has previously utilized whitepages.com, making purchases of information reportsthat the company provides. Shea previously provided **TARGET ACCOUNT #1** as the email for confirmation and signup of the Whitepages service. Based on my training, experience, and knowledge of the investigation, I believe any information purchases, requests, or other services Shea might have used to research his intended targets would have also required a confirmation email to receive the information, and Shea would have provided the **TARGET ACCOUNTS** in order to do so.

d. Shea has utilized the **TARGET ACCOUNT #1** email account in connection with other AWD operational activities. When travelling for the "Nuclear Congress" event in August 2019, he utilized the **TARGET ACCOUNT #1** email address to make bookings through Expedia.com for airfare and hotel. Shea has also purchased an AR-15 rifle kit rifle from 80lower.com, utilizing **TARGET ACCOUNT #1** as the confirmation and contact email. The rifle kit Shea purchased did not contain a lower rifle receiver but is compatible with the functional rifle lower receivers Kaleb Cole, an AWD associate and contact of Shea, possessed and was able to produce. Based on my training and experience, I believe any other purchases or orders Shea might have made online in order to plan or prepare for this operation, would have also utilized the **TARGET ACCOUNTS** and generated emails to the account.

e. Members of the private chat group also specifically discussed utilizing the Google map service in order to locate and surveil their target locations. It is known to investigators that Shea utilizes **TARGET ACCOUNT #1** and that Google Maps is one of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

services connected to the account. Shea also described in detail his plan for driving and parking nearby a target's house, and then cycling the rest of the way. Based on my training and experience, area familiarity of this nature would indicate Shea has likely already been to target locations for surveillance or reconnaissance purposes, and location data would have been captured via Location History, another Google service connected to **TARGET ACCOUNT #1**.

f. Until about July 2019, Shea used phone number 425-830-5176 as his primary phone number. Based on toll analysis and subpoena returns, it was established the 425-830-5176 phone number was disconnected and Shea assumed ownership of a new number using an Android ZTE phone with an MEID of 256691624201282613/ IMSI of 310120254586077. The Android operating system is a product of Google and is designed to have the capability to sync phone activity to a Google account. Based on my training and experience, I know that an Android device requires a Google account, and it will create a Google account unique to the MEID/IMSI of a device if no additional identifier such as a phone number or email address is provided. Subpoena returns on TARGET ACCOUNT #1 do not indicate the connection of Shea's new phone number. Since Shea utilizes an Android device that is not reflected in **TARGET ACCOUNT #1**, it is probable that **TARGET ACCOUNT #2** exists and is capable of capturing activity on Shea's Android device and connected Google services.

BACKGROUND REGARDING GOOGLE'S SERVICES

35. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access and instant messaging (otherwise known as "chat" messaging), to the general public. Google provides subscribers email and chat accounts at the domain name "[@]gmail.com." Google also allows subscribers to register a custom domain name and set up Google services such as chat and email using that domain name instead of "[@]gmail.com."

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. Subscriber Records and Account Content

36. Subscribers obtain an account by registering with Google. When doing so, email providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

37. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's websites), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

38. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation, because the information can be used to identify the account's user or users.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

39. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google servers, and then transmitted to its end destination. Google often maintains a copy of received and sent emails. Unless the sender specifically deletes an email from the Google server, the email can remain on the system indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for some period of time.

40. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

41. In addition to email and chat, Google offers subscribers numerous other services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console, Google Voice, Google+, Google Profile, Location History, Web & Activity, and YouTube, among others. Thus, a subscriber to a Google account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google Calendar is a calendar service that users may utilize to organize their schedule and share events with others. Google Drive may be used to store data and documents, including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a group or planned activity with several other remote participants. Google Photos can be used to create photo albums, store photographs, and share photographs with others and "You Tube," allows users to view, store and share videos. Google Search Console records a Google account user's search queries. And Google Web & Activity records certain browsing history depending on whether the account holder is logged into their account. Like many Internet service companies, the services Google offers are constantly changing and evolving.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

42. Based upon my training and experience, all of these types of information may be evidence of crimes under investigation. Stored emails and chats not only may contain communications relating to crimes, but also help identify the additional participants in those crimes. For example, address books and contact lists may help identify and locate co-conspirators or targets. Similarly, photographs and videos of co-conspirators may help identify their true identities, as opposed to supposed identities that they have used in telephone or email communications. Documents may identify the scope and details of the criminal activity and planning. And calendar data may reveal the timing and extent of criminal activity. Search and browsing history can also be extremely useful and may also constitute direct evidence of the crimes under investigation to the extent the browsing history or search history might include searches and browsing history related to targets, victims, locations, purchasing of supplies, and other evidence of the crimes under investigation or indications of the true identity of the account users.

43. Google is also able to provide information that will assist law enforcement in identifying other accounts associated with the **TARGET ACCOUNTS**, namely, information identifying and relating to other accounts used by the same subscriber. This information includes any forwarding or fetching accounts[2] relating to the **TARGET ACCOUNTS**, all other Google accounts linked to the **TARGET ACCOUNTS** because they were accessed from the same computer (referred to as "cookie overlap"), all other Google accounts that list the same SMS phone number as the **TARGET ACCOUNTS**, all other Google accounts that list the same recovery email addresses[3] as do the **TARGET ACCOUNTS**, and all other Google accounts that share the same creation IP address as the **TARGET ACCOUNTS**. Information associated with these associated accounts will assist law enforcement in

[2] A forwarding or fetching account related to the **TARGET ACCOUNT** would be a separate email account that can be setup by the user to receive copies of all of the email sent to the **TARGET ACCOUNT**.

[3] The recovery email address is an additional email address supplied by the user that is used by Google to confirm your username after you create an email account, help you if you are having trouble signing into your Google account or have forgotten your password, or alert you to any unusual activity involving user's Google email address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

determining who controls the **TARGET ACCOUNTS** and will also help to identify other email accounts and individuals relevant to the investigation.

B. Google Location History and Location Reporting

44. According to Google's website, "Location Reporting" allows Google to periodically store and use a device's most recent location data in connection with the Google Account connected to the device. "Location History" allows Google to store a history of location data from all devices where a user is logged into their Google Account and have enabled Location Reporting. According to Google, "[w]hen you turn on Location Reporting for a device like your iPhone or iPad, it lets Google periodically store and use that device's most recent location data in connection with your Google Account." How often Location Reporting updates location data is not fixed. Frequency is determined by factors such as how much battery life the device has, if the device is moving, or how fast the device is moving. Google's location services may use GPS, Wi-Fi hotspots, and cellular network towers to determine an account holder's location.

45. Based on the above, I know that if a user of the **TARGET ACCOUNTS** utilizes a mobile device to access the respective account identified in Attachment A and has not disabled location services on his or her device/s or through the Google account settings, Google may have detailed records of the locations at which the account holders utilized the mobile device/s. This type of evidence may further assist in identifying the account holders, and lead to the discovery of other evidence of the crimes under investigation.

46. I know that Google's Android service collects and stores identifying information about an Android smart phone used to access the Google account, including the International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), telephone number and mobile carrier code. I know that Google's Location History service periodically queries the physical location of a device that is currently accessing a Google account through the device's GPS, nearby Wi-Fi network IDs and cellular tower information and records a history of device movements in Google's servers. Because Shea is security conscious, he likely has made a concerted effort to disguise his real location, I am requesting

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Google to provide information from the Android service and Location History service from the **TARGET ACCOUNTS** in order to more accurately identify the location and phone number of the person responsible for the **TARGET ACCOUNTS**. Additionally, Location History results could provide detail as to potential target locations, and areas that have been scouted in his preparation for the operation.

C. Customer Service Communications

47. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

PRESERVATION REQUESTS

48. This evidence has not been previously available to me or other agents. On the listed dates, the FBI sent preservation letters (including renewals (*)) to the Service Provider(s) requesting that they preserve all evidence related to the accounts:

CmrnShea18[@]gmail.com (TARGET ACCOUNT #1): January 13, 2020

Any account associated with MEID 256691624201282613 / IMSI 310120254586077 (TARGET ACCOUNT #2): January 13, 2020

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

49. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit Google and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to Google with direction that it identify the account(s) described in Attachment A to this affidavit, as well as other subscriber and log records associated with the account(s), as set forth in Section I of Attachment B to this affidavit.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

50. The search warrant will direct Google to create an exact copy of the specified account(s) and records contained in the **TARGET ACCOUNTS**.

51. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

52. Analyzing the data contained in the **TARGET ACCOUNTS** may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, such as files in Google Drive, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take an extended period of time. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

CONCLUSION

53. Based on the forgoing, I request that the Court issue the proposed search warrants. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

government to search all of the items specified in Section I of Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

REQUEST FOR SEALING

54. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the target(s) of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

MICHAEL R. STULTS, Affiant
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on the 17th day of January, 2020.

BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A
GOOGLE ACCOUNTS TO BE SEARCHED

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following accounts:

CmrnShea18[@]gmail.com

Any account linked to MEID 256691624201282613 / IMSI 310120254586077

(the "**TARGET ACCOUNTS**") as well as all other subscriber and log records associated with any of the accounts, which are located at premises owned, maintained, controlled or operated by Google LLC ("Google"), an email and service provider that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B
INFORMATION TO BE SEARCHED AND SEIZED

I. Section I - Information to be disclosed by Google LLC, for search:

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC, regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account **from July 1, 2019, to the present**, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. any contact lists;

d. any downloaded Apps or Google Play purchases;

e. any Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;

f. any Google Calendar content;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. any Google Drive content (including backups of any apps stored on Google Drive;

h. any Google Sheets content;

i. any Google Forms content;

j. any Google Apps Script content;

k. any Google Maps content;

l. any Google Photos content;

m. any Google Search Console content;

n. any Google Web & Activity content;

o. any Google Chrome Sync content;

p. any Google Location History content;

q. any Google Developers Console content;

r. any Google Voice content;

s. any Android content;

t. any Google Alerts content;

u. any Google Profile content, including all Google+ content;

v. any account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

w. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

x. The types of service utilized;

y. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

z. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

This Search Warrant also requires Google to produce the following information for the Target Account (collectively the "Linked Target Accounts"):

a. a list of all other accounts linked to the **TARGET ACCOUNTS** because of cookie overlap with any **TARGET ACCOUNTS**;

b. a list of all other accounts that list the same SMS phone number as any **TARGET ACCOUNTS**;

c. a list of all other accounts that list the same recovery email address as any **TARGET ACCOUNTS**;

d. and a list of all other accounts that shared the same creation IP address as any **TARGET ACCOUNTS** within 30 days of creation;

e. Subscriber records for each of the Linked Target Accounts including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. All records and other information (not including the contents of communications) relating to the Linked Target Accounts, including:

i. Records of user activity for each connection made to or from the Account(s), including log files; messaging logs; the date time, length, and method of connections, data transfer volume; user names; and source and destination Internet Protocol Addresses; cookie IDs; browser type;

ii. Information about each communication sent or received by the Account(s), including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

iii. All records pertaining to devices associated with the accounts to include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

This Search Warrant does **not** require Google to provide any content from any of the Linked Target Accounts. Rather, the Search Warrant only requires Google to provide content for the **TARGET ACCOUNTS**.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2261(a)(2) (Stalking); 876(c) (Mailing Threatening Communications); and 371 (Conspiracy);, those violations occurring from on or about July 2019 through present, for each **TARGET ACCOUNT** listed on Attachment A, *i.e.*, the following:

a. Any information relating to the targeting of media members, Jews, or ethnic minorities;

b. Any information relating to the delivery of posters to others;

c. Any information relating to Atomwaffen;

d. Any information relating to learning the home or business addresses of members of the media, Jews, or ethnic minorities;

e. Any information relating to any threatening communications;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Information that may reveal the current or past location of the individual or individuals using the Target Accounts;

g. Information that may reveal the identities of and relationships between co-conspirators;

h. Information relating to the purchase of any items in furtherance of the conspiracy;

i. Information to establish ownership of the accounts, including information that may identify any alias names, online user names, "handles" of those who exercise in any way any dominion or control over the specified accounts as well as records or information that may reveal the true identities of these individuals;

j. Other log records, including IP address captures, associated with the specified accounts;

k. Subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

l. Records of communications between Google and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

m. Information identifying accounts that are linked or associated with the TARGET ACCOUNTS, or the Linked Target Accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of _____. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of _____, and they were made by _____ as a regular practice; and

b. such records were generated by _____'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of _____ in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by _____, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970